Towards Achieving Full Secrecy Rate in Wireless Networks: A Control Theoretic Approach

Zhoujia Mao
Department of ECE
The Ohio State University
maoz@ece.osu.edu

Can Emre Koksal
Department of ECE
The Ohio State University
koksal@ece.osu.edu

Ness B. Shroff
Departments of ECE and CSE
The Ohio State University
shroff@ece.osu.edu

Abstract*—In this paper, we consider a single-user secure data communication system. Data packets arriving at the transmitter are enqueued at a data queue to be transmitted to the receiver over a block fading channel, securely from an eavesdropper that listens to the transmitter over another independent block fading channel. We address two separate problems, both of which involve the maximization of a long-term average utility, defined as a function of the number of secure packets transmitted in each time slot. We propose a transmission controller and an admission controller based on simple index policies that do not rely on any prior statistical information on the data arrival process. The former chooses a random key generation (and transmission) rate as well as the secure data transmission rate in each time slot. Part of the data is secured by the available secrecy rate while the other part is encrypted by the key bits, enqueued at both the transmitter and the receiver. The latter chooses the amount of data admitted by the transmitter to be enqueued in the data queue. We show that our controller pair has a provably efficient performance. Also, we illustrate via simulations that the use of a key queue reduces the *queuing delay* for the data packets, while serving packets that are admitted at the maximum admissible rate. To our best knowledge, this is the first work that addresses the queuing delay in the context of secrecy.

I. Introduction

Motivated by the seminal paper by [1], there has been a large number of investigations (e.g., [2]–[8]) on wireless information theoretic secrecy. These studies have significantly enhanced our understanding of the basic limits and principles of the design and the analysis of secure wireless communication systems. Despite the significant progress in information theoretic secrecy, most of the work has focused on physical layer techniques. The application of wireless information theoretic secrecy remains mainly unresolved as it relates to the design of wireless networks and its impact on network control and protocol development. Indeed, our understanding of the interplay between the secrecy requirements and the critical functionalities of wireless networks, such as *scheduling, routing, and congestion control* remains very limited.

To that end, there have been some recent efforts to utilize the insights drawn from the aforementioned investigations on information theoretic secrecy to build secure wireless networks. In [9]–[13] the fundamental capacity and connectivity scaling laws of wireless networks with secrecy have been addressed. In [14], [15], single hop uplink scenario has been considered in which nodes enqueue arriving private and open data packets to be transmitted to a base station over block fading channels. A node is scheduled to transmit information privately from the other nodes and rate is controlled carefully to maximize an overall utility. The solution provided follows up on the stochastic network optimization framework (e.g., as treated in [16]–[19]) and generalizes the uplink scenario to incorporate *secrecy as a quality of service requirement*.

In a separate direction [20] proposed the idea of the use of a key queue in a single user system. There, a key queue is kept at the transmitter and the receiver, separately from the data queues. Instead of using the entire instantaneous secrecy rate for information transmission at all times, some of it is utilized to transmit key bits, generated randomly at the transmitter. These stored key bits are used later to secure information bits in such a way that, even when the instantaneous secrecy rate is 0, information bits can still be transmitted to the destination securely from the eavesdropper. Hence, the idea of key sharing allows one to "bank" secrecy rates at certain times to be utilized at other times. It is shown in [21] that, using this idea, a long-term *constant* secrecy rate, identical to the secrecy capacity (expected instantaneous secrecy rate) of the channel is achievable.

In this paper, we address the single user setting in the presence of arrival of data packets being enqueued at a data queue to be transmitted to the receiver over a block fading channel, securely from an eavesdropper that listens to the transmitter over another independent block fading channel. We consider two separate problems, which involve the maximization of a long-term average utility, defined as a function of the number of secure packets transmitted in each time slot. While, one would be inclined to exploit the entire secrecy rate for data transmission in each time slot in a greedy fashion, we show that this approach leads to a performance loss. Instead, the use of a key queue leads to a "smoother" secrecy rate, which in turn maximizes a concave utility, since it is negatively affected by the *second order* factors caused by the variability of the service. We propose a controller, which chooses the key generation (and transmission) rate along with the secure data transmission rate in each time slot using a transmission control component. The admission control component chooses the amount of data admitted by the transmitter to be enqueued in the data queue. These two components are based on simple index policies that do not rely on any prior statistical information on the data arrival process. We show that our

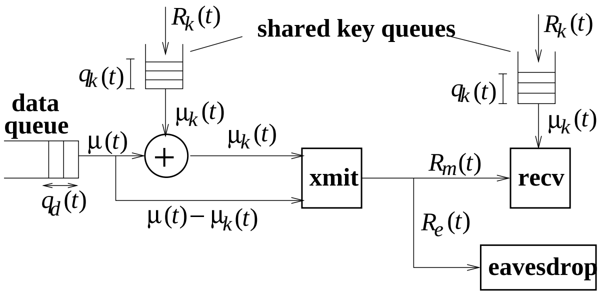

Fig. 1. System model

controller achieves a utility, arbitrarily close to the optimal utility. Also, we illustrate via simulations that the use of key queue reduces the *queuing delay* for the data packets, while serving packets that are admitted at the maximum admissible rate. To our best knowledge, this is the first work that addresses the queuing delay in the context of secrecy.

II. System Model

We consider the single-user system illustrated in Fig. 1, in which the transmitter enqueues data packets to be transmitted to the receiver over the main channel at a fixed power, securely from an eavesdropper, overhearing the transmission over a separate channel. Time is slotted, and the time-varying rates of the main and the eavesdropper channel follow general processes $\vec{R}_m = \{R_m(0), R_m(1), \ldots, R_m(T-1), \ldots\}$ and $\vec{R}_e = \{R_e(0), R_e(1), \ldots, R_e(T-1), \ldots\}$, respectively. In this paper, we assume perfect knowledge of these rates at the transmitter. We also assume the time slots are long enough and as shown in [1], the achievable instantaneous secrecy rate at a given slot t is identical to $R_s(t) = (R_m(t) - R_e(t))^+$, $\forall t \geq 0$, where $(\cdot)^+ = \max[\cdot, 0]$. In a given time slot, this rate is fully utilized: part of it is used to secure data from the data queue and the remaining part is used to transmit randomly generated key bits to be stored at the both key queues at the transmitter and the receiver. The size of the data and the key buffers are infinite.

As shown in Fig. 1, the amount of secure data transmitted at a time t is $\mu(t)$. A part ($\mu_k(t)$ bits) of this data is secured using $\mu_k(t)$ key bits by a simple bit-by-bit XOR operation. The remaining $\mu(t) - \mu_k(t)$ bits is secured using the available secrecy rate $R_s(t)$. Since the secrecy rate is fully utilized, the portion of the secrecy rate, not used to secure data is used to transmit $R_k(t)$ key bits. The data arrivals to the system is represented by the arrival process $\{A(t)\}$. The data queue state is denoted by $q_d(t)$.

The Lindley equation that models the state evolution of the key queue is:

$$q_k(t+1) = q_k(t) + R_k(t) - \mu_k(t).$$

We provide an equivalent model in the following lemma along with the constraints that specify the relationships between the parameters.

Lemma 1: The key queue q_k can be modeled with the state evolution equation $q_k(t+1) = q_k(t) + R_s(t) - \mu(t)$ with the constraints $0 \leq \mu(t) \leq \min[q_k(t) + R_s(t), R_m(t)]$, $0 \leq \mu_k(t) \leq \min[\mu(t), R_e(t)]$, and $\big(\mu(t) - \mu_k(t)\big) + R_k(t) = R_s(t)$.

Proof: We have the following relationships between the system parameters:

(1) $\mu_k(t) \leq \mu(t)$: the amount of key bits used to secure data does not exceed the amount of transmitted data.

(2) $[\mu(t) - \mu_k(t)] + R_k(t) = R_s(t)$: the instantaneous secrecy rate is fully utilized: $\mu(t) - \mu_k(t)$ is the amount of transmitted data secured over the wiretap channel in slot t and the rest of it is used to generate key bits.

(3) $\mu_k(t) \leq \min\{R_m(t), R_e(t), q_k(t) + R_k(t)\}$: the amount of used key bits cannot exceed the main channel rate, since we cannot send data at a higher rate even if all of it is secured using key bits, i.e., $\mu_k(t) \leq R_m(t)$. Also, we cannot use more key bits than the amount available in the key queue, i.e., $\mu_k(t) \leq q_k(t) + R_k(t)$. Finally, for full secrecy, the amount of shared randomness we need is no more than the eavesdropper channel rate [21]. Using more key bits will be wasteful, i.e., $\mu_k(t) \leq R_e(t)$.

Claim 1: Constraints (1), (2), and (3) imply $\mu(t) \leq R_m(t)$. If $R_m(t) \leq R_e(t)$, then $R_s(t) = 0$ and by Constraint (2), $\mu(t) = \mu_k(t) - R_k(t) \leq \mu_k(t)$. With Constraint (1), we have $\mu(t) = \mu_k(t)$, i.e., when $R_s(t) = 0$, we use key bits to secure all the data.

Likewise, from Constraint (3), we obtain $\mu(t) \leq \min\{R_m(t), q_k(t) + R_k(t)\} \leq R_m(t)$; If $R_m(t) > R_e(t)$, then $R_s(t) = R_m(t) - R_e(t)$ and by Constraint (2), $\mu(t) = R_m(t) - R_e(t) + \mu_k(t) - R_k(t) \leq R_m(t) + \mu_k(t) - R_e(t)$. Since $\mu_k(t) \leq R_e(t)$ from Constraint (3), $\mu(t) \leq R_m(t)$.

Claim 2: By Constraints (2) and (3), $\mu(t) = R_s(t) - R_k(t) + \mu_k(t) \leq q_k(t) + R_k(t) + R_s(t) - R_k(t) = q_k(t) + R_s(t)$.

Claim 3: The key state evolution is equivalent to $q_k(t+1) = q_k(t) + R_k(t) - \mu_k(t) = q_k(t) + R_s(t) - \mu(t)$ by Constraint (2).

Claim 4: Combining $\mu(t) \leq R_m(t)$ and $\mu_k(t) \leq \mu(t)$ leads to $\mu_k(t) \leq R_m(t)$.

Claims 1,2,3 and *4* complete the proof. ■

III. Problem Formulation

We consider two problems. In our **first problem**, we assume an infinitely backlogged data queue, i.e., $q_d(0) = \infty$. The objective is to maximize the long-term average utility, which is a function of the transmission rate. Our control parameters are the number, $\mu_k(t)$, of used key bits, the number, $\mu(t)$, of served data bits, and the number, $R_k(t)$, of generated key bits. In particular, we have:

$$(A) \qquad \max_{\vec{\mu}, \vec{\mu}_k, \vec{R}_k} \liminf_{T \to \infty} \frac{1}{T} \sum_{t=0}^{T-1} U(\mu(t))$$

$$\begin{aligned} \textit{s.t.} \qquad & q_k(t+1) = q_k(t) + R_s(t) - \mu(t), & (1) \\ & 0 \leq \mu(t) \leq \min[q_k(t) + R_s(t), R_m(t)], & (2) \\ & 0 \leq \mu_k(t) \leq \min[\mu(t), R_e(t)], & (3) \\ & \big(\mu(t) - \mu_k(t)\big) + R_k(t) = R_s(t), & (4) \end{aligned}$$

where the utility function $U(\cdot)$ is assumed to be monotonically increasing, reversible and differentiable on the half real line $\Re^+ \bigcup \{0\}$. Note that if there were no key queue, then we would have $q_k(t) = 0,\ \mu(t) = R_s(t),\ \mu_k(t) = 0,\ R_k(t) = 0,\ \forall t \geq 0$. Also note that, the maximum achievable average secrecy rate is upper bounded by the average secrecy capacity $\bar{R}_s = \liminf_{T \to \infty} \frac{1}{T} \sum_{t=0}^{T-1} R_s(t)$.

In our **second problem**, we assume a general data arrival process, $\{A(t)\}$ at the input of the data queue. At time t, only a portion $R(t)$ of all arrivals are admitted into the data queue in order to keep the data queue stable. All the admitted packets are required to be served by the system eventually. In the second problem, our objective is maximize the long-term average admitted data rate.

$$(B) \qquad \max_{\vec{R}, \vec{\mu}, \vec{\mu}_k, \vec{R}_k} \liminf_{T \to \infty} \frac{1}{T} \sum_{t=0}^{T-1} R(t)$$

$$\begin{aligned} \textit{s.t.} \qquad & q_d(t+1) = (q_d(t) - \mu(t))^+ + R(t), & (5) \\ & q_k(t+1) = q_k(t) + R_s(t) - \mu(t), & (6) \\ & 0 \leq R(t) \leq A(t), & (7) \\ & 0 \leq \mu(t) \leq \min[q_k(t) + R_s(t), R_m(t)], & (8) \\ & \limsup_{T \to \infty} \frac{1}{T} \sum_{t=0}^{T-1} q_d(t) < \infty, & (9) \\ & 0 \leq \mu_k(t) \leq \min[\mu(t), R_e(t)], & (10) \\ & \big(\mu(t) - \mu_k(t)\big) + R_k(t) = R_s(t). & (11) \end{aligned}$$

Note that, the maximum achievable average secrecy rate, which happens to be the objective function here, is upper bounded by the average secrecy capacity $\bar{R}_s$. As we shall show, $\bar{R}_s$ can be achieved even without a key queue. However, we will also illustrate that our solutions that involve the use of the key queue lead to smaller queueing delays, compared to the one without the key queue.

In these two problems, constraint (5) describes the data queue evolution, and constraints (1) and (6) describe the key queue evolution. Constraint (7) bounds the actual amount of sensed data $R(t)$ by the available amount of data $A(t)$ at time t. Constraints (2) and (8) state that the amount of transmitted data is bounded by both the main channel rate and the amount of keys available. Constraint (9) guarantees data queue stability. Constraints (3) and (10) state that the amount of key bits used to secure data is bounded by the eavesdropper channel rate and does not exceed the amount of transmitted data. Constraints (4) and (11) mean that the secure capacity is fully utilized by the transmission of secure data and key bits.

Virtual Queue: In order to have a fair rate allocation, we do not want the key queue to be drained frequently, which would lead to outages whenever $R_s(t) = 0$. We define $\tilde{q}_k$ as the virtual key queue and try to avoid key outage by making the virtual key queue stable (similar ideas of utilizing virtual queue are used in [19], [22]. The virtual queue evolves according to the following equation:

$$\tilde{q}_k(t+1) = \big((\tilde{q}_k(t) - \epsilon)^+ + \mu(t) - R_s(t) + \mathit{1}_o(t)\big)^+, \quad (12)$$

where $\epsilon > 0$ can be chosen arbitrarily, and

$$\begin{aligned} \mathit{1}_o(t) &= \boldsymbol{\mathit{1}}_{\textit{key queue hits zero state from higher states in slot t}} \\ &= \begin{cases} 0 & \text{if } \mu(t) = 0 \text{ or } \mu(t) < q_k(t) + R_s(t) \\ 1 & \text{otherwise} \end{cases} \end{aligned} \quad (13)$$

is the indicator that the key queue is drained in slot t. Without loss of generality, the initial state $\tilde{q}_k(0)$ can be set to be zero.

IV. Control Algorithm and Performance Analysis

In this section, we provide a simple control algorithm, analyze its performance, and show that its provably optimal for both problems described in the previous section.

A. Algorithm

Our algorithm for Problem (A) involves only a transmission rate controller. The transmission controller attempts to provide a smooth service by the help of the key bits.

Transmission Control (TC): We define $V \in \Re^+$ to be the control parameter of our algorithm. In slot t, the controller solves the following optimization problem and transmits with the calculated rate:

$$\max_{\mu(t) \in \Pi(t)} \frac{V}{2} U(\mu(t)) - \tilde{q}_k(t)\mu(t), \quad (14)$$

where $\Pi(t) = \{\mu(t) : 0 \leq \mu(t) \leq \min[q_k(t) + R_s(t), R_m(t)]\}$ is a compact and nonempty set. Furthermore, key generation and usage rates $(R_k(t), \mu_k(t))$ are chosen as follows: If $\mu(t) > R_s(t)$, then $R_k(t) = 0$ and $\mu_k(t) = \mu(t) - R_s(t)$; if $\mu(t) \leq R_s(t)$, then $\mu_k(t) = 0$ and $R_k(t) = R_s(t) - \mu(t)$. This ensures that constraint $\big(\mu(t) - \mu_k(t)\big) + R_k(t) = R_s(t)$ is satisfied. It is not surprising that $\mu_k(t) R_k(t) = 0$, since any solution with $\mu_k(t) > 0$ and $R_k(t) > 0$, can be equivalently replicated by using the secrecy rate to transmit data rather than generating and using key bits at the same time. Note that $R_s(t) = \big(R_m(t) - R_e(t)\big)^+ \geq R_m(t) - R_e(t)$, then for $\mu(t) > R_s(t)$, we have $\mu_k(t) = \mu(t) - R_s(t) \leq R_m(t) - R_s(t) \leq R_e(t)$. This leads to constraint $0 \leq \mu_k(t) \leq \min[\mu(t), R_e(t)]$ being satisfied.

The set, $\Pi(t)$ of possible data transmission guarantees constraint (2) on $\mu(t)$ in Problem (A). If $U(\cdot)$ is concave, the objective function is a concave function of $\mu(t)$. Consequently, *TC* solves a simple convex optimization problem in each time slot. The positive term $\frac{V}{2} U(\mu(t))$ can be viewed as a utility obtained from the transmission rate $\mu(t)$ and the term $\tilde{q}_k(t)\mu(t)$ can be viewed as its associated cost. When the virtual key queue $\tilde{q}_k(t)$ is small, *TC* tries to allocate a high amount of transmitted data to increase the utility; and when

$\tilde{q}_k(t)$ is large, *TC* allocates a small amount of transmitted data to reduce cost. This pushes the served data rate to be smoother over time. It is also notable that (14) involves *only* $\mu(t)$. The key generation and usage rates are not part of this optimization, and are chosen subsequently.

In Problem (B), we need to control both the admission and transmission rate such that the admitted rate is maximized while keeping the data queue stable. In our algorithm, there are two components: a *admission control* component and a *transmission control* component. The transmission control component is the identical to the one described above for Problem (A), and the admission control component is as follows:

Admission Control (AC): In slot t, the controller solves the following optimization problem and admit the calculated amount of data arrivals:

$$\max_{0 \leq R(t) \leq A(t)} \frac{V}{2} U(R(t)) - q_d(t) R(t), \tag{15}$$

Both *TC* and *AC* are *index policies*, i.e., the solutions are memoryless and they depend only on the instantaneous values of the system variables.

B. Performance Analysis

Recall that $A(t)$ is the original data arrival and $R(t)$ is the amount of data admitted to the data queue. The natural question one would ask here is, whether our admission controller rejects too many packets in the first place to *synthetically* keep the data queue stable. In the following theorem, we show that this is not the case. Indeed, the admission rate associated with *AC* and *TC* can be made closer to the optimum by increasing the control parameter V. We use the notation $y = O(x)$ to represent y going to 0 as x goes to 0.

Theorem 1: If
1) $U(\cdot)$ is strictly concave on $\Re^+ \bigcup \{0\}$, and its slope at 0 satisfies[1] $0 \leq \beta = U'(0) < \infty$,
2) $0 \leq \limsup_{T\to\infty} \frac{1}{T}\sum_{t=0}^{T-1} A^2(t) < \infty$ and $0 \leq R_m(t) \leq R_{max} < \infty$, $\forall t \geq 0$,
then *TC* achieves:

$$\liminf_{T\to\infty} \frac{1}{T}\sum_{t=0}^{T-1} U(\mu(t)) \geq \liminf_{T\to\infty} \frac{1}{T}\sum_{t=0}^{T-1} U(\mu^*(t)) - O(\frac{1}{V}), \tag{16}$$

and *AC* achieves:

$$q_d(t) \leq \beta\frac{V}{2}, \quad \forall\, t \geq 0 \tag{17}$$

$$\liminf_{T\to\infty} \frac{1}{T}\sum_{t=0}^{T-1} U(R(t)) \geq \liminf_{T\to\infty} \frac{1}{T}\sum_{t=0}^{T-1} U(R^*(t)) - O(\frac{1}{V}), \tag{18}$$

$$\liminf_{T\to\infty} \frac{1}{T}\sum_{t=0}^{T-1} R(t) \to \liminf_{T\to\infty} \frac{1}{T}\sum_{t=0}^{T-1} R^*(t) \;\; as \;\; V \to \infty, \tag{19}$$

where $\vec{\mu}^* = \{\mu^*(0), \mu^*(1), \ldots, \mu^*(T-1), \ldots\}$ and $\vec{R}^* = \{R^*(0), R^*(1), \ldots, R^*(T-1), \ldots\}$ are the optimal solutions to Problem (A) and Problem (B), respectively.

The proof of Theorem 1 can be found in Appendix A. Equation (17) shows that the data queue q_d is stable. In Equation (16), the gap between the average transmission rate with our algorithm and the optimal average transmission rate can be made arbitrarily small by choosing parameter V large. Similarly, by Equation (19), the admission rate can be close to optimum with large V. As a tradeoff, the data queue length increases as V increases. From Equation (18), we observe that, if we plug the rates allocated by our algorithm in the utility function, it still remains close to the utility achieved by the optimal solution of Problem (B). This implies that, *AC* and *TC* allocate rates smoothly over time, as opposed to the case without a key queue. Based on this observation, combined with Equation (16), we expect the queueing delay to be smaller with a key queue. We will verify this in the following numerical example.

V. Numerical Example

In this section we simulate our algorithms and numerically compare them with the optimal performance. In the simulation, the number of time slots is $T = 10^6$. We use the utility function $U(x) = \log_2(1 + x)\ \forall x \geq 0$. The main channel rate is uniformly distributed over $[0, 100]$ and the eavesdropper channel rate is uniformly distributed over $[0, 50]$. As a result of the simulation, the average secure capacity $\bar{R}_s = 29.1$. We also set the virtual key queue parameter $\epsilon = 0.01$.

We first use an arrival process $A(t),\ t \geq 0$, that is composed of independent Poisson random variables with mean 30 each slot. In this example, $\bar{A} > \bar{R}_s$. We run the simulation for different values of the control coefficient V and compare the results with the optimal value[2]. In Figure 2(a), one can observe that, as V increases, the average utility of the transmission rate with a key queue approaches the optimal value, which is consistent with Equation (16). For the case without a key queue, the average utility remains a constant and is quite smaller. Figure 2(b) shows that, as V increases, the average admission rate (both with and without a key queue) also increases to the optimum, which is consistent with Equation (19). As a tradeoff, the average queue length increases but remains bounded as shown in Figure 2(c). Although the optimal admission rate can be approached both with and without a key queue, the delay performance with a key queue is better as we can see in Figure 2(d).

Figure 3 illustrates the same scenario, with a more bursty arrival process. This time, $A(t) = 0$ w.p. $\frac{1}{2}$ and $A(t) = 50$ w.p. $\frac{1}{2}$ independently for each time slot. Consequently, $\bar{A} = 25 < \bar{R}_s$. Similar observations to the previous case can be made with this arrival process.

[1] For instance, $U(1 + R) = \log(1 + R)$.

[2] Note that the optimal value for Problem (A) is $U(\bar{R}_s)$ and for Problem (B) is $\min[\bar{A}, \bar{R}_s]$.

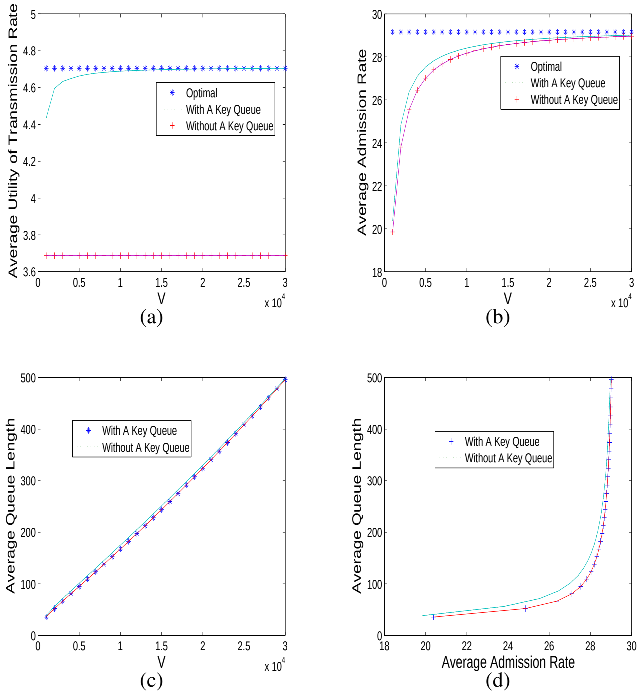

Fig. 2. Performance Evaluation of *TC* and *AC* with respect to the solutions of Problem (A) and (B) under Poisson Arrivals: (a) Control Parameter V vs. Average Utility of Transmission Rate; (b) Control Parameter V vs. Average Admission Rate; (c) Control Parameter V vs. Queueing Delay; (d) Throughput vs. Delay Curve

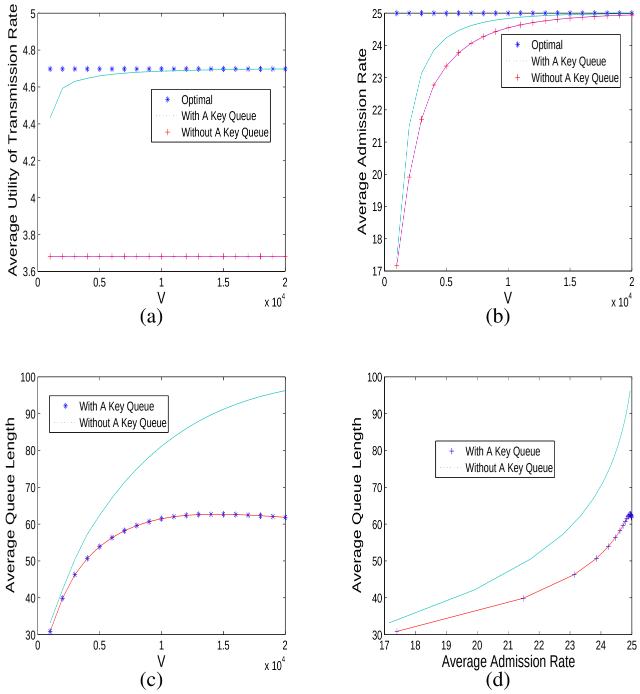

Fig. 3. Performance Evaluation of *TC* and *AC* for Problem (A) and (B) under Variable Arrivals

VI. Conclusion

In this paper, we considered a single-user secure data communication system and addressed two separate problems, both of which involve the maximization of a long-term average utility, defined as a function of the number of secure packets transmitted in each time slot. We proposed a transmission controller and an admission controller based on simple index policies that do not rely on any prior statistical information on the data arrival process. We showed that our controller pair has a provably efficient performance. Also, we illustrated via simulations that the use of a key queue reduces the *queuing delay* for the data packets, while serving packets that are admitted at the maximum admissible rate. This is due to the fact that, the transmission controller is designed to choose the rate of served packets as uniformly over time as possible.

References

[1] A. Wyner, “The Wire-Tap Channel,” *The Bell System Technical Hournal*, vol. 54, no. 8, pp. 1355–1387, October 1975.

[2] P. K. Gopala, L. Lai, and H. El Gamal, “On the secrecy capacity of fading channels,” vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[3] J. Barros and M. R. D. Rodrigues, “Secrecy capacity of wireless channels,” in *Proc. IEEE Int. Symposium Inform. Theory*, Seattle, WA, July 2006, pp. 356–360.

[4] D. Gunduz, R. Brown, and H. V. Poor, “Secret communication with feedback,” in *Proc. IEEE Intl. Symposium on Information Theory and its Applications*, Auckland, New Zealand, Dec. 2008.

[5] A. Khisti and G. W. Wornell, “Secure transmission with multiple antennas: The MISOME wiretap channel,” *IEEE Trans. Inform. Theory*, 2009, to appear.

[6] Y. Liang, H. V. Poor, and S. Shamai (Shitz), “Secure communication over fading channels,” *IEEE Trans. Inform. Theory*, vol. 54, no. 6, pp. 2470–2492, June 2008.

[7] E. Ekrem and S. Ulukus, “The secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel,” Mar. 2009, submitted.

[8] M. Yuksel, X. Liu, and E. Erkip, “A secure communication game with a relay helping the eavesdropper,” Taormina, Italy, Oct. 2009, to appear.

[9] O. O. Koyluoglu, C. E. Koksal, and H. E. Gamal, “On secrecy capacity scaling in wireless networks,” 2010, submitted.

[10] ——, “On the effect of colluding eavesdroppers on secrecy scaling,” in *Proceedings of European Wireless, EW*, Lucca, Italy, 2010.

[11] S. Goel, V. Aggarwal, A. Yener, and A. R. Calderbank, “Modeling location uncertainty for eavesdroppers: A secrecy graph approach,” Austin, TX, June 2010.

[12] S. Vasudevan, D. Goeckel, and D. F. Towsley, “Security-capacity trade-off in large wireless networks using keyless secrecy,” Chicago, IL, September 2010.

[13] A. Sarkar and M. Haenggi, “Secrecy coverage,” Pacific Grove, CA, Nov. 2010.

[14] C. E. Koksal and O. Ercetin, “Control of wireless networks with secrecy,” in *”Asilomar Conference on Signals, Systems, and Computers”*, Pacific Grove, CA, Nov. 2010.

[15] C. E. Koksal, O. Ercetin, and Y. Sarikaya, “Control of wireless networks with secrecy,” *CoRR*, vol. abs/1101.3444, 2011.

[16] L. Tassiulas and A. Ephremides, “Jointly optimal routing and scheduling in packet ratio networks,” *IEEE Transactions on Information Theory*, vol. 38, no. 1, pp. 165 –168, Jan. 1992.

[17] X. Liu, E. K. P. Chong, and N. B. Shroff, “A framework for opportunistic scheduling in wireless networks,” *Computer Networks*, vol. 41, no. 4, pp. 451–474, 2003.

[18] A. Stolyar, “Greedy primal-dual algorithm for dynamic resource allocation in complex networks,” *Queueing Systems*, vol. 54, pp. 203–220, 2006, 10.1007/s11134-006-0067-2. [Online]. Available: http://dx.doi.org/10.1007/s11134-006-0067-2

[19] M. Neely, “Energy Optimal Control for Time Varying Wireless Networks,” *IEEE Transactions on Information Theory*, vol. 52, no. 7, pp. 2915–2934, July 2006.

[20] K. Khalil, M. Youssef, O. O. Koyluoglu, and H. El Gamal, “On the delay limited secrecy capacity of fading channels,” Seoul, Korea, June - July 2009.

[21] O. Gungor, J. Tan, C. E. Koksal, H. El Gamal, and N. B. Shroff, “Joint power and secret key queue management for delay limited secure communication,” San Diego, CA, March 2010.

[22] Z. Mao, C. Koksal, and N. Shroff, "Resource Allocation in Sensor Networks with Renewable Energy," in *Proc. of the 19th International Conference on Computer Communication Networks*, 2010.

APPENDIX

A. Proof of Theorem 1

Proof of Equation (17): Equation (17) directly follows from the following lemma:

Lemma 2: Under algorithm *AC* and *TC*, we have

$$q_d(t) \le \frac{\beta V}{2}, \quad \tilde{q}_k(t) \le \frac{\beta V}{2}.$$

Proof: Since $U(\cdot)$ is concave on $\Re^+ \bigcup \{0\}$, we have $U(\mu(t)) \le U(0) + \beta\mu(t)$, $\forall t \ge 0$, where $0 \le \beta = U'(0) < \infty$. Then, $\frac{V}{2}U(\mu(t)) - \tilde{q}_k(t)\mu(t) \le \frac{V}{2}U(0) + \frac{\beta V}{2}\mu(t) - \tilde{q}_k(t)\mu(t)$ where $\mu(t)$ is the solution of *TC*.

If $\frac{\beta V}{2}\mu(t) - \tilde{q}_k(t)\mu(t) < 0$, then we get $\frac{V}{2}U(\mu(t)) - \tilde{q}_k(t)\mu(t) < \frac{V}{2}U(0)$. However, *TC* chooses $\mu(t)$ that maximizes $\frac{V}{2}U(\mu(t)) - \tilde{q}_k(t)\mu(t)$ which means $\frac{V}{2}U(\mu(t)) - \tilde{q}_k(t)\mu(t) \ge \frac{V}{2}U(0)$ since $0 \in \Pi(t)$. Then, we must have $\frac{\beta V}{2}\mu(t) - \tilde{q}_k(t)\mu(t) \ge 0$, i.e.,

$$\tilde{q}_k(t)\mu(t) \le \frac{\beta V}{2}\mu(t). \tag{20}$$

We now prove the result by induction. Without loss of generality, let $\tilde{q}_k(0) \le \frac{\beta V}{2}$. Suppose for all $t \ge 1$, $\tilde{q}_k(t-1) \le \frac{\beta V}{2}$ holds. In slot t, if $\mu(t) = 0$, then $\tilde{q}_k(t) \le \tilde{q}_k(t-1) \le \frac{\beta V}{2}$ by Equation (12). Otherwise, $\mu(t) \ne 0$, and by Equation (20), we have $\tilde{q}_k(t) \le \frac{\beta V}{2}$.

$q_d(t) \le \frac{\beta V}{2}$ can be obtained using the same argument. ∎

Proof of Equation (16): We define the Lyapunov function $L(\tilde{q}_k(t)) = (\tilde{q}_k(t))^2$, and $\Delta(\tilde{q}_k(t)) = L(\tilde{q}_k(t+1)) - L(\tilde{q}_k(t))$. From Equation (12), we have

$$\begin{aligned}\big(\tilde{q}_k(t+1)\big)^2 \le& \big(\tilde{q}_k(t) - \epsilon\big)^2 + \big(\mu(t) - R_s(t) + 1_o(t)\big)^2 + \\ & 2\big(\tilde{q}(t) - \epsilon\big)^+\big(\mu(t) - R_s(t) + 1_o(t)\big) \\ \le& \big(\tilde{q}_k(t)\big)^2 + \epsilon^2 + \big(1 + R_{max}\big)^2 + 2\epsilon R_{max} + \\ & 2\tilde{q}_k(t)1_o(t) + 2\tilde{q}_k(t)\mu(t) - 2\tilde{q}_k(t)R_s(t),\end{aligned}$$

then

$$\begin{aligned}\Delta =& \Delta(\tilde{q}_k(t)) \\ \le& VU(\mu(t)) - VU(\mu(t)) + \epsilon^2 + \big(1 + R_{max}\big)^2 + 2\epsilon R_{max} \\ & + 2\tilde{q}_k(t)1_o(t) + 2\tilde{q}_k(t)\mu(t) - 2\tilde{q}_k(t)R_s(t) \\ \le& VU(\mu(t)) + \epsilon^2 + \big(1 + R_{max}\big)^2 + 2\epsilon R_{max} + \beta V 1_o(t) \\ & - 2\left[\frac{V}{2}U(\mu(t)) - \tilde{q}_k(t)\mu(t)\right] - 2\tilde{q}_k(t)R_s(t).\end{aligned}$$

It is apparent that *TC* is trying to maximize the value of the term $\big[\frac{V}{2}U(\mu(t)) - \tilde{q}_k(t)\mu(t)\big]$. Since the optimal solution for Problem (A) may not be unique, we let $\mathcal{U}^*$ be the optimal solution set and $\mu^* \in \mathcal{U}^*$ be any optimal solution, for Problem (A) given any sample path. Since the constraint set $\Pi(t)$ is queue dynamic related, it is possible that $\mu^*(t) \notin \Pi(t)$.

Lemma 3: In slot t, if by solving *TC*, we get $\big[\frac{V}{2}U(\mu(t)) - \tilde{q}_k(t)\mu(t)\big] < \big[\frac{V}{2}U(\mu^*(t)) - \tilde{q}_k(t)\mu^*(t)\big]$, then $\mu(t) < \mu^*(t)$ and $1_o(t') = 1$ for some $t' \le t$ and $t - t' < \infty$.

Proof: In time slot t, let $\mu^m(t)$ be the value that maximize the unconstrained objective function $\frac{V}{2}U(\mu(t)) - \tilde{q}_k(t)\mu(t)$.

Claim 1: $q_k(t) + R_s(t) \le R_m(t)$. Otherwise, $\Pi(t) = [0, R_m(t)]$ which is not queue dynamic related, then $\big[\frac{V}{2}U(\mu(t)) - \tilde{q}_k(t)\mu(t)\big] \ge \big[\frac{V}{2}U(\mu^*(t)) - \tilde{q}_k(t)\mu^*(t)\big]$.

Claim 2: $\mu^m(t), \mu^*(t) > q_k(t) + R_s(t)$. If $\mu^m(t), \mu^*(t) \in \Pi(t)$, we must have $\big[\frac{V}{2}U(\mu(t)) - \tilde{q}_k(t)\mu(t)\big] \ge \big[\frac{V}{2}U(\mu^*(t)) - \tilde{q}_k(t)\mu^*(t)\big]$, then $\mu^*(t) > q_k(t) + R_s(t)$. If $\mu^m(t) < 0$, we will have $\frac{V}{2}U(0) = \big[\frac{V}{2}U(\mu(t)) - \tilde{q}_k(t)\mu(t)\big] \ge \big[\frac{V}{2}U(\mu^*(t)) - \tilde{q}_k(t)\mu^*(t)\big]$, then $\mu^m(t) > q_k(t) + R_s(t)$.

By the above claims, $\mu(t) < \mu^*(t)$ and $\mu(t) < \mu^m(t)$. Suppose $\mu(t) < q_k(t) + R_s(t)$, since the objective function of *TC* is concave in $\mu(t)$, we can increase $\mu(t)$ to increase the objective without violating the constraint. Thus, $\mu(t) = q_k(t) + R_s(t)$ and $1_o(t) = 1$. It is also possible that $1_o(t') = 1$ for some $t' < t$ and $R_s(\tau) = 0$, $\forall \tau \in [t', t]$. Note that $t - t' < \infty$, otherwise, $\limsup_{T\to\infty} \frac{1}{T}\sum_{t=0}^{T-1} R_s(t) = 0$. ∎

Let $N = \max\{n :$ *for any* $t \ge 0,\ R_s(\tau) = 0,\ \forall \tau \in [t, t+n]\}$. By using Lemma 3 and $\mu(t), \mu^*(t) \le R_m(t) \le R_{max}$, $\forall t \ge 0$, we have $N < \infty$ and

$$\begin{aligned}\Delta \le& VU(\mu(t)) - VU(\mu^*(t)) + \epsilon^2 + \big(1 + R_{max}\big)^2 + 2\epsilon R_{max} \\ & + 2\tilde{q}_k(t)\Big[\mu^*(t) - R_s(t)\Big] + V(\beta + NU(R_{max}))1_o(t).\end{aligned} \tag{21}$$

Lemma 4:

$$\frac{1}{V}\limsup_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1}\tilde{q}_k(t)[\mu^*(t) - R_s(t)] \le O(\frac{1}{V}).$$

Proof: Note that

$$\sum_{t=0}^{T-1}\mu^*(t) - \left[q_k(0) + \sum_{t=0}^{T-1}R_s(t)\right] \le 0,$$

then

$$\sum_{t=0}^{T-1}\Big(\mu^*(t) - R_s(t) - \delta\Big) < q_k(0),$$

where δ can be arbitrarily small. By divided by T and taking $\limsup_{T\to\infty}$ of both sides, we have

$$\limsup_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1}\Big(\mu^*(t) - R_s(t) - \delta\Big) < 0. \tag{22}$$

Construct an auxiliary queue with the following evolution:

$$\bar{q}_k^*(t+1) = \Big(\bar{q}_k^*(t) - R_s(t) - \delta\Big)^+ + \mu^*(t),$$

then with Equation (22), $\bar{q}_k^*(t)$ is strongly stable. By multiplying $\tilde{q}_k(t)$ for both sides of the inequality $\bar{q}_k^*(t+1) \ge \bar{q}_k^*(t) - R_s(t) - \delta + \mu^*(t)$ and rearranging terms, we obtain

$\tilde{q}_k(t)\Big[\mu^*(t) - R_s(t)\Big] \le \tilde{q}_k(t)\Big[\bar{q}^*_k(t+1) - \bar{q}^*_k(t) + \delta\Big]$. By summing from 0 to $T-1$, dividing by T and taking $\limsup_{T\to\infty}$, we have

$$
\begin{aligned}
&\frac{1}{V}\limsup_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1}\tilde{q}_k(t)[\mu^*(t) - R_s(t)] \\
\le&\frac{1}{V}\limsup_{T\to\infty}\frac{1}{T}\sum_{t=1}^{T}\bar{q}^*_k(t)\big(\tilde{q}_k(t-1) - \tilde{q}_k(t)\big) \\
&+\frac{1}{V}\limsup_{T\to\infty}\frac{\tilde{q}_k(T)\bar{q}^*_k(T) - \tilde{q}_k(0)\bar{q}^*_k(0)}{T} \\
&+\limsup_{T\to\infty}\frac{1}{T}\sum_{t=1}^{T}\frac{\tilde{q}_k(t)}{V}\delta \\
\le&\frac{R_{max}+\epsilon}{V}\limsup_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1}\bar{q}^*_k(t) + \frac{\delta}{V}\frac{\beta V}{2} \\
=&O(\frac{1}{V}) + \frac{\delta\beta}{2},
\end{aligned}
$$

since the average queue length of the auxiliary queue remains stable and is not related to V. By letting $\delta \to 0$, we finish the proof. ■

Lemma 5: If $\tilde{q}_k(t) \le \frac{\beta V}{2}$, then $q_k(t) < \infty$.

Proof: First, we provide a rough idea of the proof: by exploring the relations between $\tilde{q}_k(t)$ and $q_k(t)$, we notice that as $q_k(t)$ increases from 0 to at most $\beta\frac{V}{2}$, $\tilde{q}_k(t)$ will hit zero at some slot. Once $\tilde{q}_k(t)$ becomes zero, *TC* results in $\mu(t) = \min[q_k(t) + R_s(t), R_m(t)]$. Since $R_s(t) \le R_m(t)$, $q_k(t)$ will either be zero or decrease. We now give the proof details.

Without loss of generality, let $q_k(0) = 0$. We have the following cases:

i) if $\mu(t) \ge R_s(t)$, $I_o(t) = 0$ and $\tilde{q}_k(t) > 0$, then $q_k(t+1) \le q_k(t)$ and $\tilde{q}_k(t+1) - \tilde{q}_k(t) \le q_k(t) - q_k(t+1)$, i.e., even if $\tilde{q}_k(t)$ increases, the increment is no larger than the decrement of $q_k(t)$;

ii) if $\mu(t) < R_s(t)$, $I_o(t) = 0$, then if $\tilde{q}_k(t+1) > 0$, $\tilde{q}_k(t) - \tilde{q}_k(t+1) \ge q_k(t+1) - q_k(t)$, i.e., the decrement of $\tilde{q}_k(t)$ is no less than the increment of $q_k(t)$, else if $\tilde{q}_k(t+1) = 0$, it goes to case iv);

iii) if $I_o(t) = 1$, then $q_k(t+1) = 0$ by Equation (1) and Equation (13);

iv) if $\tilde{q}_k(t) = 0$, by Equation (14), *TC* chooses $\mu(t) = \min[q_k(t) + R_s(t), R_m(t)]$, then either $q_b(t+1) = 0$, or $q_k(t+1) = q_k(t) - R_m(t) + R_s(t) \le q_k(t)$.

From the above discussion, we have $q_k(t) \le \beta\frac{V}{2} < \infty$. ■

Lemma 6: If both the key queue $q_k(t)$ and virtual key queue $\tilde{q}_k(t)$ are strongly stable, i.e.,

$$
\limsup_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1}\big(q_k(t) + \tilde{q}_k(t)\big) < \infty,
$$

then $\limsup_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1} I_o(t) \le \epsilon$.

Proof: Using the idea similar to [19], we have the fact that if any queue represented with $Q(t)$ is strongly stable, then $\limsup_{T\to\infty}\frac{Q(T)}{T} = 0$. Hence, if $q_k(t)$ and $\tilde{q}_k(t)$ are strongly stable, $\limsup_{T\to\infty}\frac{q_k(T)}{T} = \limsup_{T\to\infty}\frac{\tilde{q}_k(T)}{T} = 0$. From Equation (12), we have

$$
\tilde{q}_k(t+1) \ge \tilde{q}_k(t) - \epsilon + I_o(t) + \mu(t) - R_s(t).
$$

Note that $q_k(t+1) = q_k(t) - \mu(t) + R_s(t)$. By adding from 0 to $T-1$, dividing by T and taking $\limsup$ on both sides, we have

$$
\begin{aligned}
\limsup_{T\to\infty}\frac{\tilde{q}_k(T)}{T} \ge \lim_{T\to\infty}\frac{\tilde{q}_k(0)}{T} - \epsilon + \limsup_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1} I_o(t) \\
+ \lim_{T\to\infty}\frac{q_k(0) - q_k(T)}{T}.
\end{aligned}
$$

Since $\limsup_{T\to\infty}\frac{\tilde{q}_k(T)}{T} = \lim_{T\to\infty}\frac{\tilde{q}_k(0)}{T} = \lim_{T\to\infty}\frac{q_k(0)}{T} = \lim_{T\to\infty}\frac{q_k(T)}{T} = 0$, so we get $\limsup_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1} I_o(t) \le \epsilon$. ■

By summing from 0 to $T-1$, dividing by T and V, taking $\liminf_{T\to\infty}$ over Equation (21), combined with Lemma 2, Lemma 5, Lemma 6, and Lemma 4, we get

$$
\begin{aligned}
\liminf_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1}U(\mu(t)) \ge& \liminf_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1}U(\mu^*(t)) - O(\frac{1}{V}) \\
&- \epsilon(NU(R_{max}) + \beta). \quad ■
\end{aligned}
$$

By letting $\epsilon \to 0$, we obtain Equation (16).

Proof of Equation (18) and Equation (19): We define $L(q_d(t)) = (q_d(t))^2$, and $\Delta(q_d(t)) = L(q_d(t+1)) - L(q_d(t))$. By Equation (5), we have

$$
\begin{aligned}
\Delta =&\Delta(q_d(t)) \\
\le& VU(R(t)) - 2\left[\frac{V}{2}U(R(t)) - q_d(t)R(t)\right] + A^2(t) + R^2_{max} \\
&- 2q_d(t)\mu(t) \qquad (23)
\end{aligned}
$$

$$
\begin{aligned}
&(P1) \qquad \max_{\vec{R}}\liminf_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1}R(t) \\
&(P2) \qquad \max_{\vec{R}}\liminf_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1}U(R(t)) \\
&s.t. \qquad q_d(t+1) = (q_d(t) - \mu(t))^+ + R(t), \\
&\qquad\qquad 0 \le R(t) \le A(t), \\
&\qquad\qquad \limsup_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1}\big[R_s(t) - \mu(t)\big] = 0, \\
&\qquad\qquad \limsup_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1}q_d(t) < \infty,
\end{aligned}
$$

Lemma 7: (P1) and (P2) have different objective functions under the same set of constraints. Let $\vec{R}^*$ be the maximizer of (P2), then it is also the maximizer of (P1).

Proof: Suppose there exists $\vec{R}^*_1$ such

$$
\liminf_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1}R^*(t) < \liminf_{T\to\infty}\frac{1}{T}\sum_{t=0}^{T-1}R^*_1(t),
$$

then there exists $\vec{R}_2^*$ such that $R^*(t) \leq R_2^*(t) \leq A(t),\ \forall t \geq 0$ and

$$\begin{aligned}\liminf_{T\to\infty} \frac{1}{T}\sum_{t=0}^{T-1} R^*(t) <& \liminf_{T\to\infty} \frac{1}{T}\sum_{t=0}^{T-1} R_2^*(t)\\ \leq& \liminf_{T\to\infty} \frac{1}{T}\sum_{t=0}^{T-1} R_1^*(t).\end{aligned}$$

i.e., there are infinitely many slots in which $R^*(t) - R_2^*(t) < 0$. Since $U(\cdot)$ is strictly concave, $U(R^*(t)) - U(R_2^*(t)) < \beta_m(R^*(t) - R_2^*(t)) < 0$ if $R^*(t) - R_2^*(t) < 0$, where $0 < \beta_m = \min\{\frac{U(R^*(t))-U(R_2^*(t))}{R^*(t)-R_2^*(t)} :\ R^*(t) - R_2^*(t) < 0\}$. Thus,

$$\liminf_{T\to\infty} \frac{1}{T}\sum_{t=0}^{T-1} U(R^*(t)) < \liminf_{T\to\infty} \frac{1}{T}\sum_{t=0}^{T-1} U(R_2^*(t)),$$

which contradicts the fact that $\vec{R}^*$ is the maximizer of (P2). ■

Note that $q_k(t+1) = q_k(t) + R_s(t) - \mu(t)$. By Lemma 5, we have the fact that *TC* results into

$$\limsup_{T\to\infty} \frac{1}{T}\sum_{t=0}^{T-1} \big[R_s(t) - \mu(t)\big] = 0, \tag{24}$$

then Problem (B) is reduced to (P1). By Lemma 7, $\vec{R}^*$ is also the maximizer of Problem (B). Substituting $R^*(t)$ into Equation (23), we obtain

$$\begin{aligned}\Delta \leq& VU(R(t)) - VU(R^*(t)) + A^2(t) + R_{max}^2\\ &+ 2q_d(t)\Big[R^*(t) - \mu(t)\Big].\end{aligned}$$

Note that $\limsup_{T\to\infty} \frac{1}{T}\sum_{t=0}^{T-1} \big[R^*(t) - R_s(t))\big] \leq 0$ and $\limsup_{T\to\infty} \frac{1}{T}\sum_{t=0}^{T-1} A^2(t) < \infty$. combining with Equation (24) and using the same idea as in Lemma 4, we have

$$\frac{1}{V}\limsup_{T\to\infty} \frac{1}{T}\sum_{t=0}^{T-1} q_d(t)[R^*(t) - \mu(t)] \leq O(\frac{1}{V}).$$

Then, we further obtain

$$\liminf_{T\to\infty} \frac{1}{T}\sum_{t=0}^{T-1} U(R(t)) \geq \liminf_{T\to\infty} \frac{1}{T}\sum_{t=0}^{T-1} U(R^*(t)) - O(\frac{1}{V}),$$

where $\vec{R}^*$ is the maximizer of (P2), (P1) and Problem (B). This equation also means that as $V \to \infty$, $\vec{R}$ becomes the maximizer of (P2). By applying Lemma 7 again, we have

$$\liminf_{T\to\infty} \frac{1}{T}\sum_{t=0}^{T-1} R(t) \to \liminf_{T\to\infty} \frac{1}{T}\sum_{t=0}^{T-1} R^*(t)\ \textit{as}\ V \to \infty. \quad ■$$